西安電子科技大學
XIDIAN UNIVERSITY

Aalto University
School of Electrical
Engineering

Achieving Trustworthy Cyber Systems: Challenges and Strategies

Trust Management Enhanced Security with Privacy

Zheng Yan (闫峥)

Xidian University & Aalto University

zyan@xidian.edu.cn; zheng.yan@aalto.fi

14 December, 2017

Outline

Background

Background

- Trust Management
  - Evaluating, establishing, controlling, enhancing and ensuring trust – a solution in system level
  - Facilitate collaboration among system entities
    - Centralized, distributed or mobile environments
    - Traditional security paradigms cannot be enforced
  - Trust evaluation
    - Collect and analyze data related to trust and calculate a trust value by considering factors influencing trust

Enablers

Evaluation: probability theories, data analytics, data mining, etc.
Establishment: cryptography and security schemes, etc.
Control: control mechanisms & theories (subjective policy)
Enhancement: privacy, risk & identity management
Usability: usable security and human-computer trust interaction
QoS, energy efficiency – reliability, …
Assurance: all above and more

Characteristics of Cyber Systems

- Cyber Systems
  - Large scale and heterogeneity (supported by different computer network infrastructure and communication platforms)
  - Hybrid and dynamic topology or structure: Distributed + Centralized -> dynamically changed or switched
  - Lack trust among system entities (e.g., IoT)
  - Big data related
  - Vulnerable: attacks and vulnerabilities – hard to detect all and protect accordingly
  - Hard to apply centralized control or management for all system layers and entities
    - Different operators, different owners, different expectation and various requirements in different contexts

Challenges on Trust Management

Establishment: efficiency, scalability, adaptability
Control: context-aware and personalization
Enhancement: privacy, robustness, & identity management, trustworthiness
Applicability: user acceptance and economic view (lack study)
Assurance: all above and more

Typical Cyber Systems

- Cloud Computing
  - Large scale
  - Centralized
  - Cannot be fully trusted
  - Big data related
  - DoS/DDoS attacks and intrusions
- Pervasive Social Networking
  - Heterogeneity
  - Hybrid topology
  - Lack trust among system entities
  - Big data related
  - Vulnerable
  - Hard to apply centralized control or management
- Apply trust management to enhance security with the concern of privacy preservation

Trust Management in Cloud Computing

- Cloud data access control based on trust and reputation
- Encrypted cloud data deduplication with access control
- Secure computation on encrypted cloud data
- Verifiable computation
- Cloud QoS management (based on adaptive trust control model)

Background

Cloud Computing

- Provide seemingly unlimited resources
- Enable scalability, elasticity, fault-tolerance, and pay-per-use

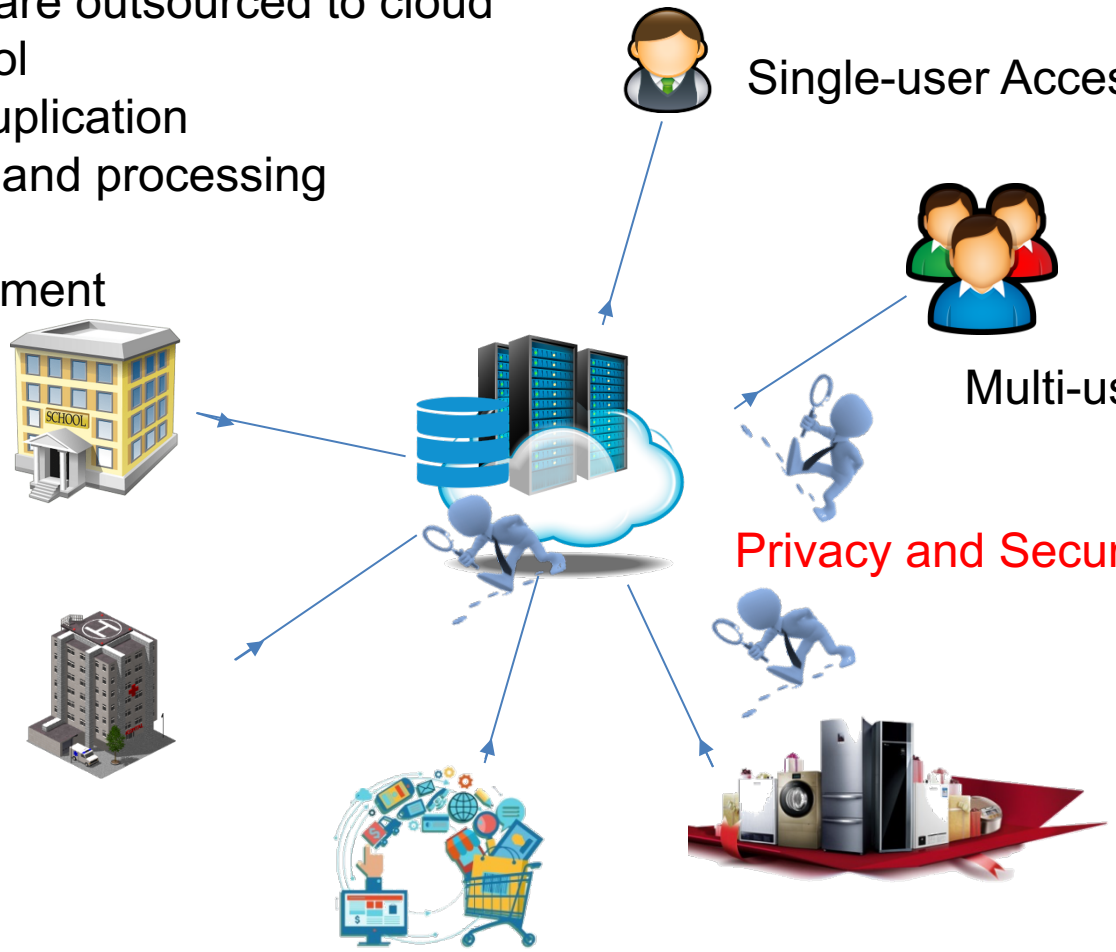
Data Outsourcing

- Break the bottlenecks of restricted local resources
- Release the heavy burden of cloud users
- Complete complicated computation and storage mission

Research Motivation

Encrypted data are outsourced to cloud

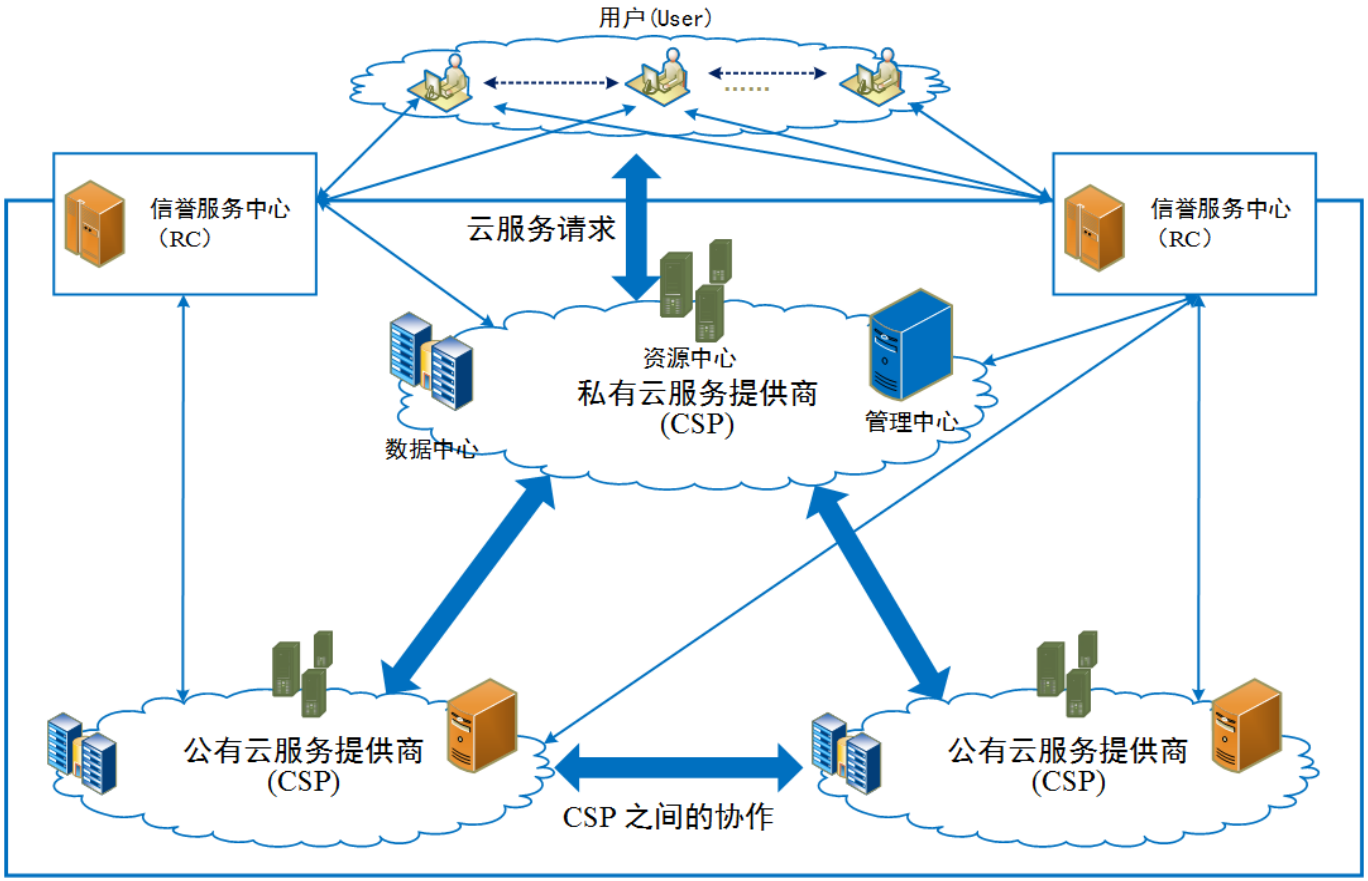
- Access control
- Storage Deduplication
- Computation and processing
- Verification
- QoS management



Cloud Service Provider cannot be fully trusted!

Cloud Data Access Control based on Trust and Reputation

- L.J. Gao, Z. Yan*, L.T. Yang "Game Theoretical Analysis on Acceptance of a Cloud Data Access Control System Based on Reputation", IEEE Transactions on Cloud Computing, 2016. Doi: 10.1109/TCC.2016.2632110.
- Z. Yan*, X.Y. Li, M.J. Wang, A.V. Vasilakos, “Flexible Data Access Control based on Trust and Reputation in Cloud Computing”, IEEE Transactions on Cloud Computing, pp. 485-498, 2017. Doi: 10.1109/TCC.2015.2469662
- Z. Yan*, W.Y. Shi, “CloudFile: A Cloud Data Access Control System based on Mobile Social Trust”, Journal of Network and Computer Applications, Vol. 86, pp. 46-58, May 15, 2017.
- Z. Yan*, X.Y. Li, R. Kantola, “Controlling Cloud Data Access Based on Reputation", Mobile Networks and Applications, Springer, 20(6), pp. 828-839, December 2015. Doi: 10.1007/s11036-015-0591-6. (IF: 1.496/2015)



Three Schemes

Cloud data access control based on social trust (mobile users);

Cloud data access control based on reputation (RC)

Cloud data access control based on either above or both

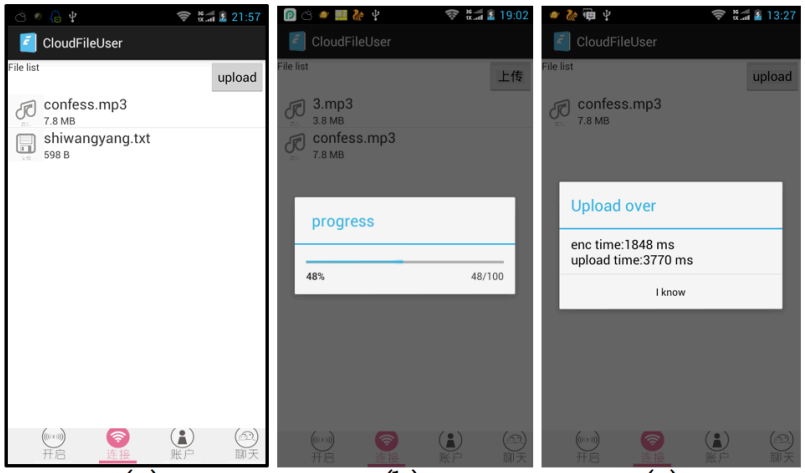


Fig. 3. File upload: (a) file upload UI; (b) upload processing progress; (c) upload success UI with recorded file encryption time and uploading time

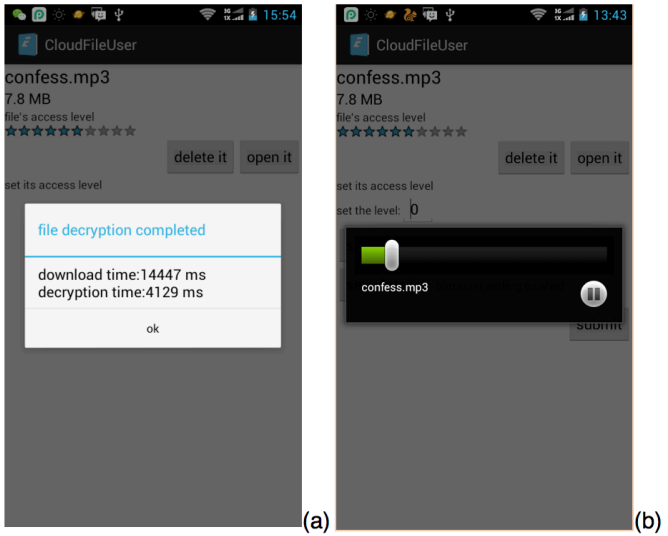


Fig. 6. Access and download a file from cloud server

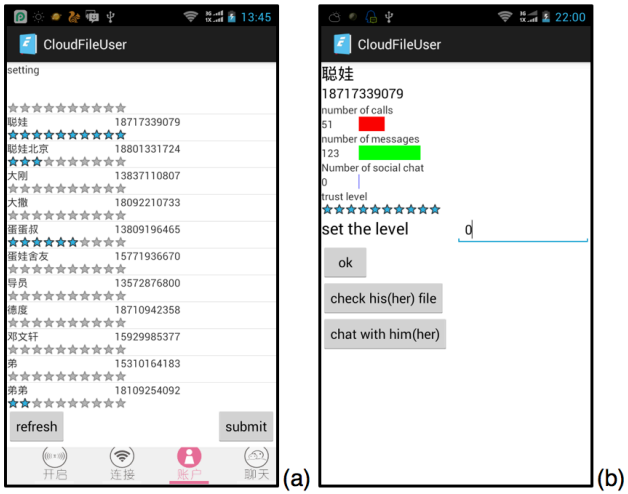


Fig. 7. (a) Personal contact list with social trust values; (b) Details of mobile social networking statistics of a contact with its cloud data access link

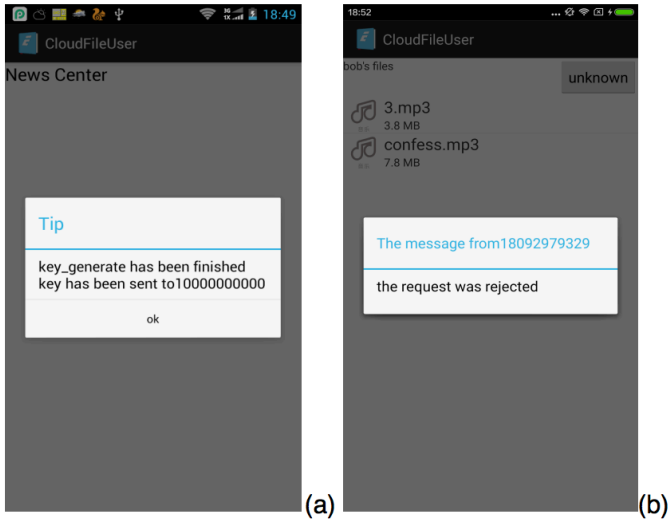


Fig. 10. (a) File access key generation and issuing; (b) File access rejection

Encrypted Data Deduplication

- Zheng Yan, Wenxiu Ding, Xixun Yu, Haiqi Zhu, and Robert H. Deng, "Deduplication on encrypted big data in cloud", *IEEE Transactions on Big Data*, vol.2, no.2, pp. 138-150, 2016. (**The 2017 IEEE ComSoc TCBD Best Journal Paper Award**)
- Zheng Yan, Lifang Zhang, Wenxiu Ding, Qinghua Zheng, "Heterogeneous Data Storage Management with Deduplication in Cloud Computing", IEEE Transactions on Big Data, 2017. Doi: 10.1109/TBDATA.2017.2701352
- Zheng Yan, Mingjun Wang, Yuxiang Li, A.V. Vasilakos, "Encrypted Data Management with Deduplication in Cloud Computing", IEEE Cloud Computing Magazine, 3(2), pp. 28-35, 2016.
- Wenxiu Ding, Zheng Yan, Robert H. Deng. Secure Encrypted Data Deduplication with Ownership Proof and User Revocation[C]. *ICA3PP 2017*, Helsinki, Finland, LNCS 10393, Springer, pp. 297-312, 2017.

Schemes of Encrypted Data Deduplication

- Encrypted data deduplication with data owner offline by employing Proxy Re-encryption
- Encrypted data deduplication with data owner online by employing Attribute based Encryption
  - No need a third trusted party support
- Encrypted data deduplication with either data owner offline or online or both
  - A flexible and hybrid solution
- Encrypted data deduplication with efficient ownership proof and user revocation
  - Data owner offline support
  - Less interaction with the server

Encrypted Data Computations

- Wenxiu Ding, Zheng Yan, and Robert H. Deng. Encrypted Data Processing with Homomorphic Re-Encryption[J]. *Information Sciences*, 2017, vol. 409, pp. 35-55.
- Wenxiu Ding, Zheng Yan, and Robert H. Deng. Privacy-Preserving Data Processing with Flexible Access Control[J]. Submitted to *IEEE Transactions on Dependable and Secure Computing*. (Minor Revision)

Research Issues

- High cost introduced by FHE
- Hard to support computations over a large number of data
- Limited computations enabled by PHE
- Do not consider the access control over processing result for multiple users

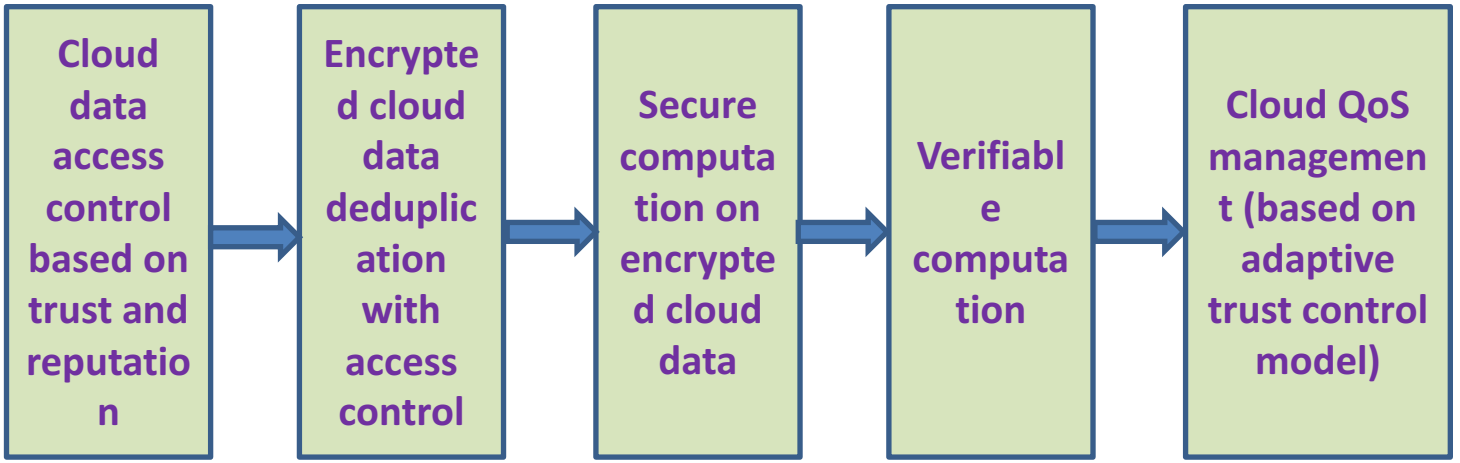
Schemes of Encrypted Data Computation

- Encrypted Data Processing with Homomorphic Re-Encryption
  - Combine the features of homomorphism and re-encryption
  - Split secret key and issue them to two non-colluding servers
  - Contributions: High efficiency; Computation over a big number of provided data; Flexibility (Homo-Re-Encryption); 7 operators
- Privacy-Preserving Data Processing with Flexible Access Control
  - Take advantage of the homomorphism of Attribute-Based Encryption (ABE)
  - Split keys and share them to two non-colluding servers
  - Contributions
    - High efficiency for multi-user access
    - Computation over a big number of provided data
    - Secure and fine-grained access control over the result of encrypted data processing

Verifiable Computation & QoS Management

- X.X. Yu, Z. Yan*, A.V. Vasilakos, “A Survey of Verifiable Computation”, Mobile Networks and Applications, Springer, 22(3), pp. 438-453, June 2017. Doi: 10.1007/s11036-017-0872-3 (IF: 3.259)
- Z. Yan*, X.X. Yu, W.X. Ding, “Context-Aware Verifiable Cloud Computing”, IEEE Access, Vol. 5, pp. 2211 – 2227, Feb. 9 2017. Doi: 10.1109/ACCESS.2017.2666839 (IF: 3.224)
- W. Tang, Z. Yan*, “CloudRec: A Mobile Cloud Service Recommender System based on Adaptive QoS Management”, IEEE TrustCom/BigDataSE/ISPA, vol. 1, pp. 9-16, 2015.

Trust Management in Cloud Computing

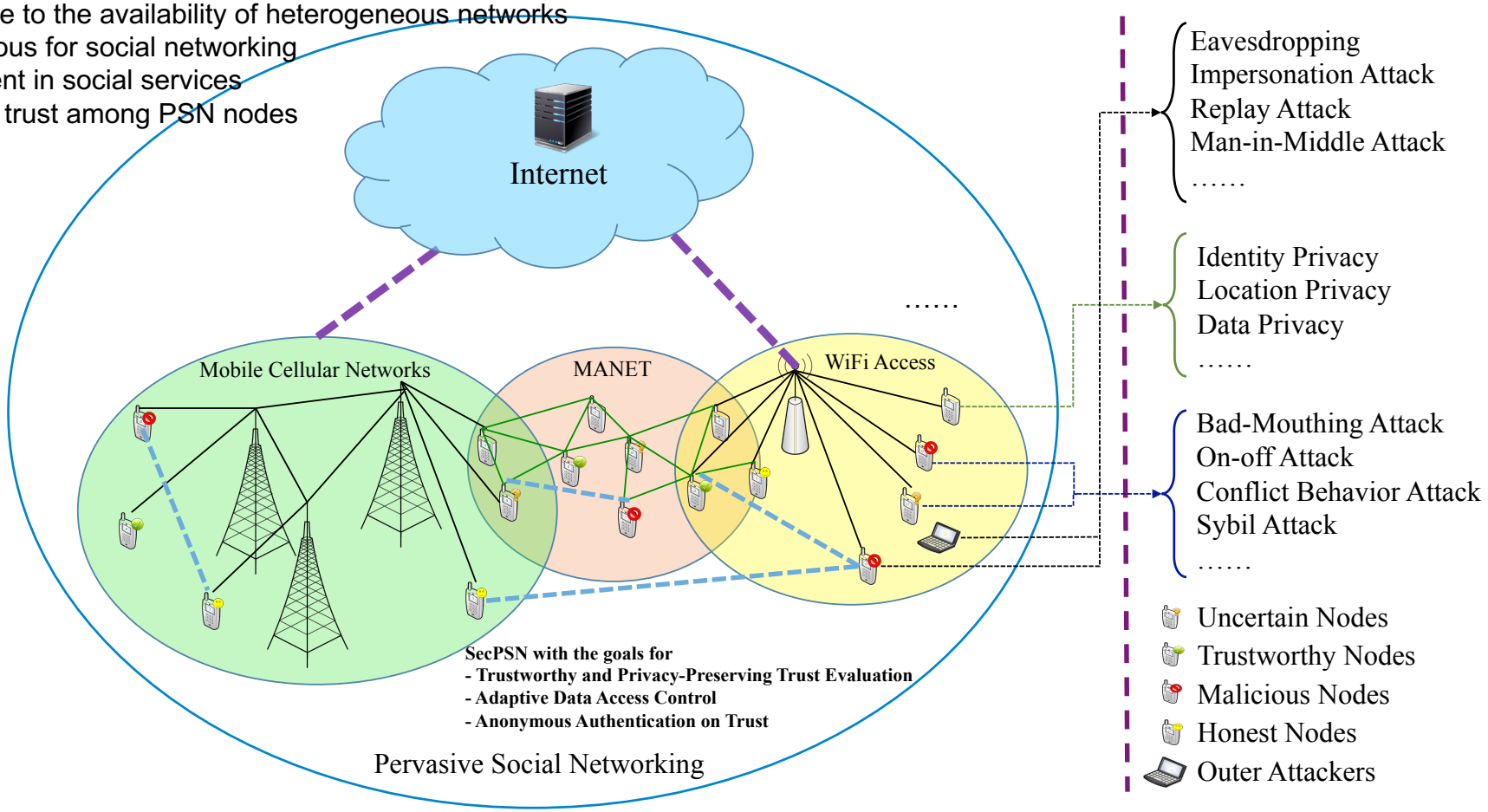


Trust Management in Pervasive Social Networking

- PSN data access control based on multi-dimensional trust levels
- Anonymous authentication on trust
- Unwanted content control in PSN based on trust management
- Trustworthy and privacy preserving trust evaluation

Digitalizing Trust for Securing Pervasive Social Networking with Privacy Preservation

Adaptive to the availability of heterogeneous networks
Ubiquitous for social networking
Intelligent in social services
Lack of trust among PSN nodes



Pervasive Social Networking (PSN) offers instant social activities at anytime and anywhere with the support of heterogeneous networks

Trustworthy and Privacy-Preserving Trust Evaluation

- Zheng Yan, Wenxiu Ding, Valtteri Niemi, and Athanasios V. Vasilakos. Two Schemes of Privacy-Preserving Trust Evaluation[J]. *Future Generation Computer Systems*, vol.62, pp. 175-189, 2016.

Research Issues

- Privacy concerns of data providers
- Encryption incurs high computational cost
- Difficult to identify faked evidence (internal attacks)
- Difficult to employ complicated trust evaluation model
- The reliability of trust evaluation results

Design Basis of Schemes

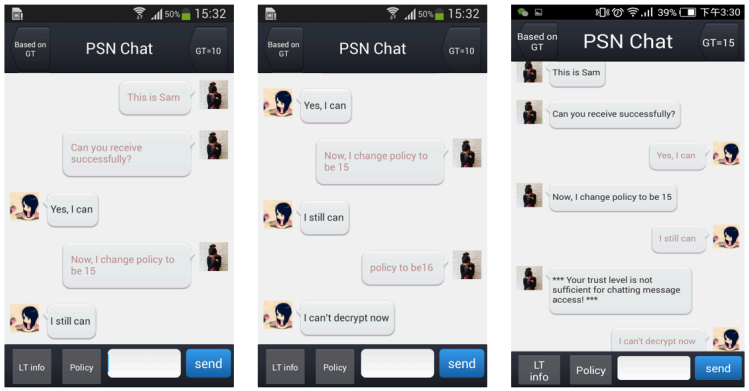
- Collect encrypted evidence to preserve user privacy
- Apply time decaying function, deviation function and trimmed mean method to resist attacks
- Use Rayleigh cumulative distribution function models the impact of the number of collected evidences

PSN Data Access Control based on Trust

- N. Li, Z. Yan*, M. J. Wang, L. T. Yang, “Securing Communication Data in Pervasive Social Networking based on Trust with KP-ABE”, ACM Trans. on Cyber-Physical Systems, 2017. (accepted)
- Z. Yan*, M.J. Wang, “Protect Pervasive Social Networking based on Two Dimensional Trust Levels”, IEEE Systems Journal, Vol. 11, Issue 1, pp. 207-218, March 2017. Doi: 10.1109/JSYST.2014.2347259. (IF: 3.882)
- C.Y. Huang, Z. Yan*, N. Li, M. J. Wang, “Secure Pervasive Social Communications based on Trust in a Distributed Way”, IEEE Access, vol. 4, pp. 9225 – 9238, Jan. 4, 2017. Doi: 10.1109/ACCESS.2017.2647824 (IF: 3.224)

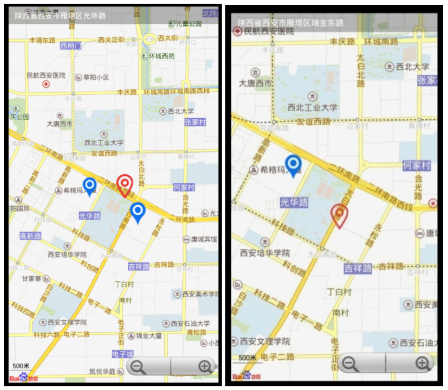
PSN Data Access Control

Apply either the trust evaluated by PSN nodes or the reputation evaluated by a server or both to flexibly control PSN communication data access



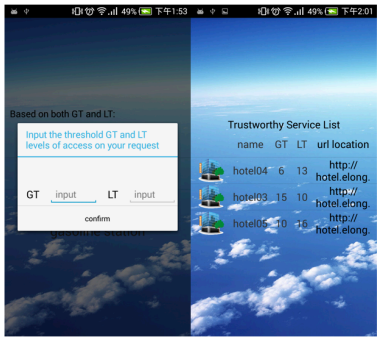
(a) (b) (c)

Fig. 14: (a) Phone A's screenshot; (b) Phone A's screenshot; (c) Phone B's screenshot



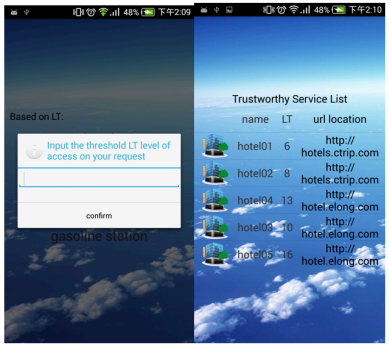
Node 1 Node 3

Fig.16. GPS locations showed in Node 1 and Node 3



(a) (b)

Fig. 11. (a) Service access policy based on GT and LT; (b) The result list of services with policy $GT \geq 5$ *and* $LT \geq 10$



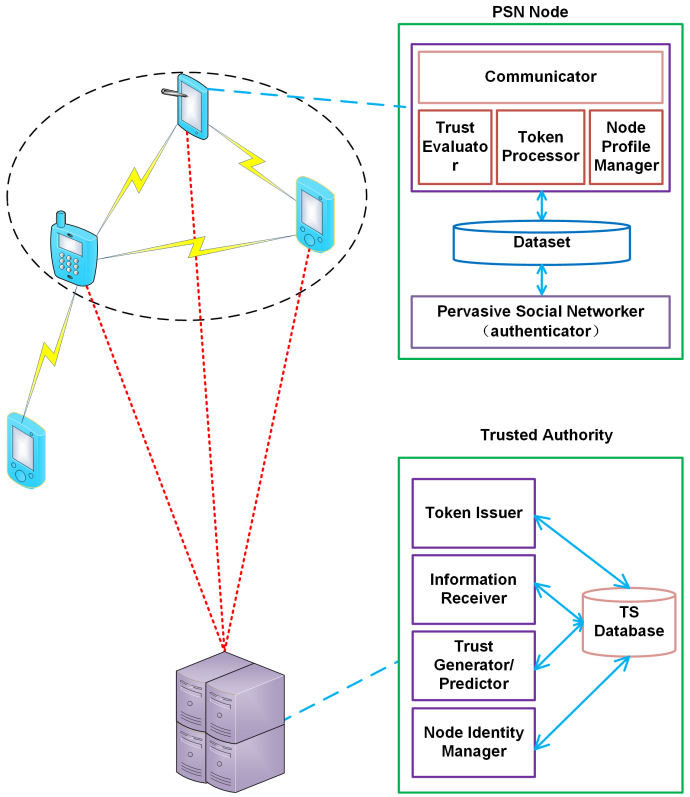
(a) (b)

Fig. 12. (a) Service access policy based on LT; (b) The result list of services with policy $LT \geq 5$

Anonymous Authentication on Trust

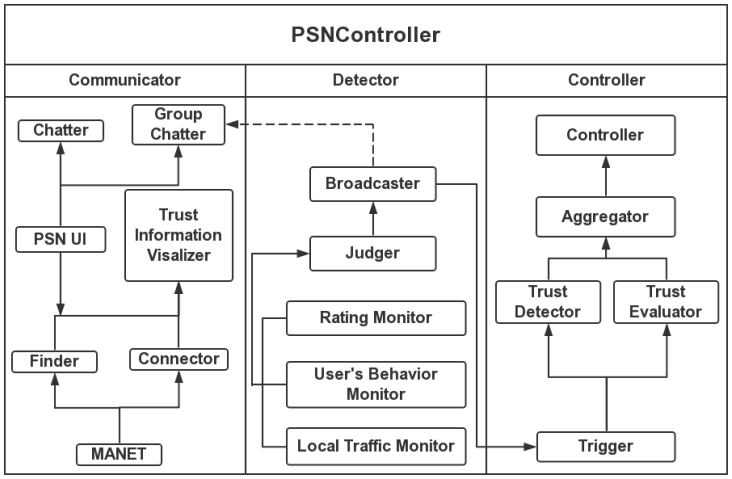
- Z. Yan*, W. Feng, P. Wang, “Anonymous Authentication for Trustworthy Pervasive Social Networking”, IEEE Transactions on Computational Social Systems, 2(3), pp. 88-98, Feb. 2016. Doi: 10.1109/TCSS.2016.2519463
- W. Feng, Z. Yan*, H.M. Xie, "Anonymous Authentication on Trust in Pervasive Social Networking Based on Group Signature", IEEE Access, Vol. 5, Issue 1, pp. 6236-6246, 2017. Doi: 10.1109/ACCESS.2017.2679980 (IF: 3.224)
- Z. Yan*, P. Wang, W. Feng, “A Novel Scheme of Anonymous Authentication on Trust in Pervasive Social Networking”, Information Sciences, minor revision.

- Anonymous Authentication on Trust in Pervasive Social Networking
  - Bilinear pairing
  - Certificateless authentication
  - Centralized solution based on a Trusted Authority that issues trust values of PSN nodes
- Anonymous Authentication on Trust in Pervasive Social Networking Based on Group Signature
  - Depend on a trusted server as a group manager
- Anonymous Authentication on Trust in Pervasive Social Networking to support any number of trust authority
  - A semi-distributed solution
  - The trust values of TA or PSN nodes can be authenticated in an anonymous ways

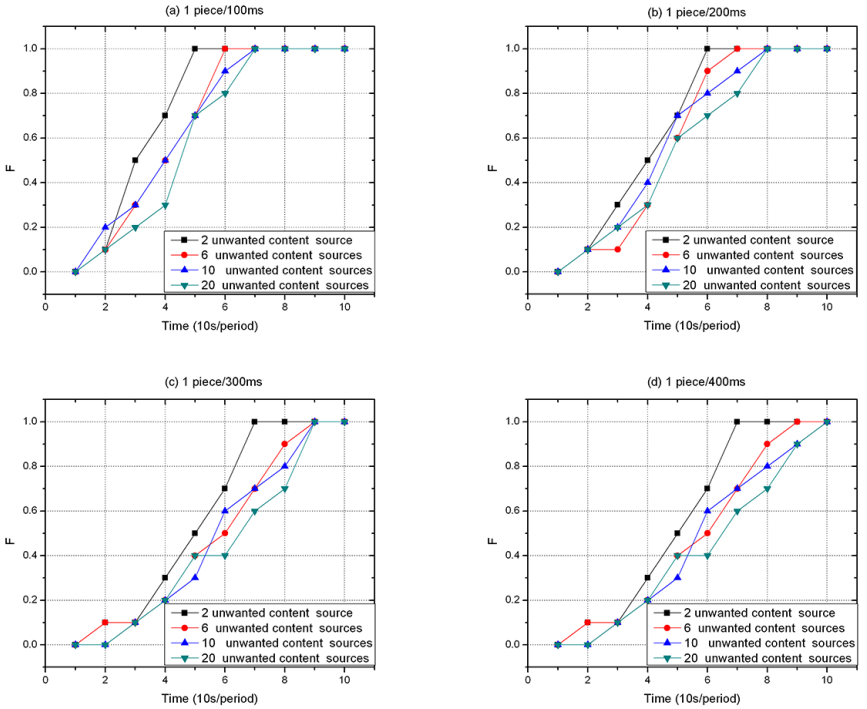


Unwanted Content Control based on Trust Management

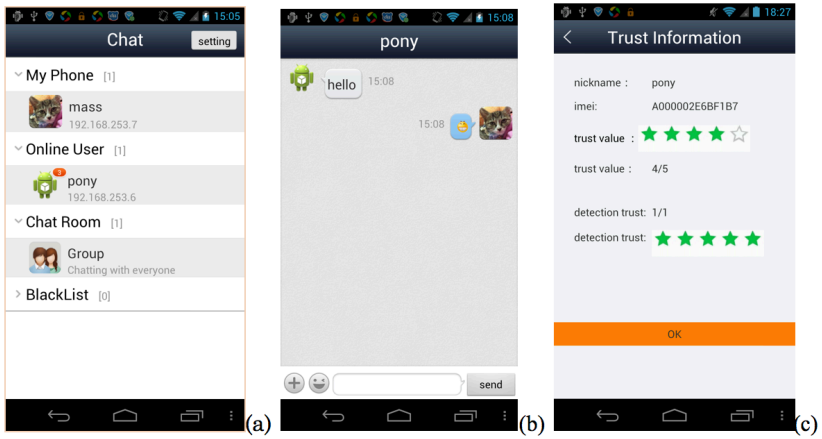
- S.X. Ma, **Z. Yan***, “PSNController: An Unwanted Content Control System in Pervasive Social Networking based on Trust Management”, ACM Transactions on Multimedia Computing Communications and Applications, 12, 1s, Article 17, October 2015, 23 pages.



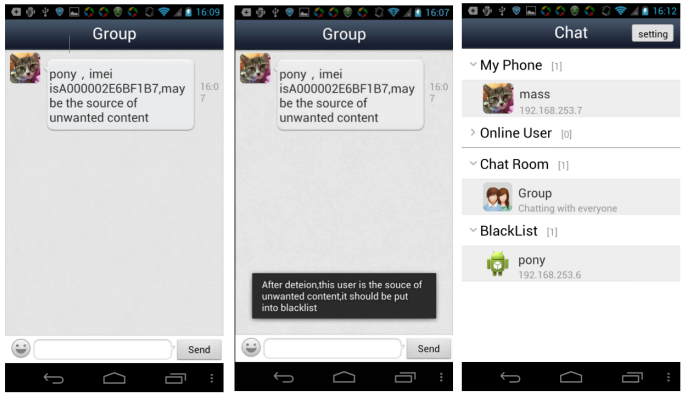
Prototype Structure



Unwanted Content Detection Accuracy

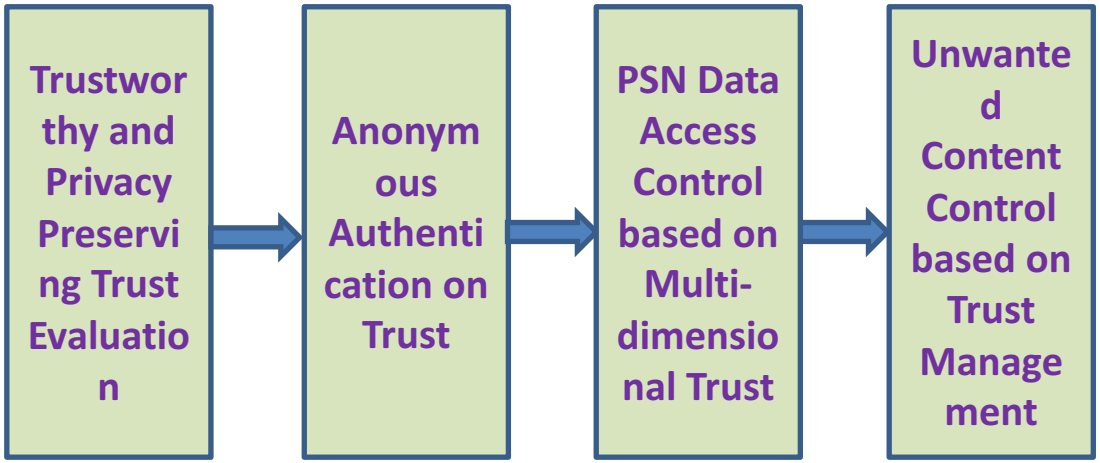


Prototype UI



A process to control the source of unwanted contents

Trust Management in Pervasive Social Networking



Challenges and Strategies

Challenges

Use trust management to enhance security with privacy preservation

1. How to fuse and process big data for trust evaluation with trustworthiness and privacy preservation?
2. How to manage trust in a decentralized way?
3. How to ensure user acceptance?
4. How to ensure adaptability, scalability, and efficiency? (in a mobile environment)

Strategies

Use trust management to enhance security with privacy preservation

1. Big data based trust evaluation with efficient and effective fusing and processing capability, attack detection capability, privacy preserving capability
2. An effective and secure technology for decentralized trust management with a proper incentive mechanism? (ensure trust behaviors)
3. Study user acceptance from the view of economy and user profits?
4. Study context-aware solutions, research technologies across-domain and across-layer, investigate light-weight solutions

Conclusion and Future Work

- ✓ Research of trust management enhanced security with privacy preservation
  - ✓ Cloud computing
  - ✓ Pervasive social networking
- ✓ Research challenges and strategies for trustworthy cyber systems
- ✓ Future work
  - ✓ Decentralization
  - ✓ Trust evaluation based on big data

Thanks!

Q&A